IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Bruce Wallace, et al.	Examiner:	N. Patel
Serial No.:	10/615,513	Art Unit:	2435
Conf. No.:	9214		
Filed:	July 8, 2003	Attorney Docket No.:	15929ROUS02U
Title:	DISTRIBUTED SECURITY FOR INDUSTRIAL NETWORKS		

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being filed electronically on October 22, 2009.

/John C. Gorecki/

John C. Gorecki, Reg. No. 38,471

M.S. Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

This reply brief is being filed in response to the Examiner's answer dated August 31, 2009. This reply brief is being filed to further explain the operation of the cited references to narrow the issues for appeal.

As summarized in the Appeal Brief, this application relates to a way in which access, to particular PLCs and attendant factory machines, may be circumscribed so that a person using a management program is not automatically allowed to access all PLCs on the network.

Claim 1 recites, in relevant part:

> a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network…

When this claim is parsed, it is clear that:

1. the SPIP is "connected between the local area network and the one or more programmable logic controllers;

2. the SPIP isolates the one or more programmable logic controllers from the local area network; and
3. the SPIP prevents a person using a management program from accessing the one or more programmable logical controllers over the local area network

The combination of prior art references does not teach or suggest a SPIP of this nature that is connected in this manner or that performs these functions.

The Examiner has explained, in section (10) of the Examiner's Answer (see Examiner's Answer at page 13-15) that Hamilton teaches a management program that enables a user to access programmable logic controllers via a local area network. (Examiner's Answer at page 14, lines 2-16). The Examiner further explains that this management program includes one or more security layers that provide user authentication, authorization, and policy. (Examiner's Answer at page 14, lines 16-21 and drawing at page 15).

In the Examiner's drawing (see Examiner's Answer at page 15), the Examiner has assumed a client/server model in which the client-side program is being used (e.g. on a PC) and the access tool 20 is running on a network-based server. The Examiner has interpreted the client side application as the "management program" and the server side (access tool) as the SPIP. Applicants agree that this is one way that the Access tool 20 of Hamilton may be implemented. In this embodiment, as drawn by the Examiner, the client-side interactions would occur over the network as noted by the Examiner. However, the portion the Examiner omitted to note, in this drawing, was that the interaction between the access tool and the box labeled "Industrial Control Components(s) PLC(s)" also occurs over the network. Specifically, the "access tool" is server-based and instantiated in a server that sits on the network. It does not physically reside between the PLCs and the local area network as drawn by the Examiner. For example, a quick comparison of the Examiner's figure with Fig. 1 of Hamilton reveals that the real-time interactions between the "access tool 20" and the "Industrial Component(s) 24) occurs on network 30. (see also Hamilton at col. 4, lines 60-61 "An access tool 20 interacts with one or more industrial components 24 via a network 30.")

This omitted reference to the local area network in-between the access tool and the programmable logical controllers is important for several reasons. For example, claim 1 recites that the SPIP is connected between the local area network and the one or more programmable logic controllers. The access tool 20 in Hamilton is clearly not "connected between" the

programmable logic controllers and the network, since Figure 1 of Hamilton clearly shows the programmable logic controllers connected directly to the network, and that the network is used to carry communications between the programmable logic controllers and the access tool 20. Thus, if the access tool 20 of Hamilton is interpreted to be the SPIP, the access tool fails to meet this limitation of claim 1.

Further, claim 1 recites that the SPIP isolates the one or more programmable logic controllers from the local area network. The Examiner has focused on the fact that the access tool has one or more security layers. However, regardless of the number of security layers, the access tool 20 does not perform the claimed function of isolating the programmable logic controllers from the local area network, because it uses the local area network to communicate with the programmable logic controllers.

Finally, the Examiner has interpreted the client system as the "management program" and the access tool as the "SPIP". (See Examiner's Answer at page 14 lines 21-22 and page 15 lines 1-3). The Examiner then asserts that the access tool (server) prevents the management program (client) from taking action on the programmable logic controllers. However, as is well known in the computer arts, a client cannot take action without the server. Hence, the client (management program) couldn't have accessed the programmable logic controllers with the server. In this environment, the server is not preventing the client from accessing the PLCs, since the client can't do that on its own.

Stated differently, in a client/server s software architecture a client interacts with a server to cause the server to take particular actions. The client does not actually perform the functions but rather instructs the server to implement particular functions. Claim 1 recites that the SPIP prevents "a person using a management program from accessing the one or more programmable logic controllers..." This implies that the management program is actually capable of accessing the one or more programmable logic controllers. A client software component without the associated server portion would not be able to actually implement any of the management functions since the client software component does not do the functions but rather causes the server to implement the functions. Thus, the "client" in Hamilton cannot be reasonably interpreted to be the "management software" since it is only part of the management software. Rather, a more natural reading of Hamilton is that the client side software and the server side (access tool) together are the management software that is used by a user to interact with the

programmable logic controllers. This management software has security layers that require the user to log into the management system before taking action through the management system. When the user launches the management client, the client interacts with the access tool and that combined interaction enables the user to interact with the programmable logic controllers. The Examiner's attempt to split the client portion from the server portion and call one the "management program" and the other the "security policy implementation point" was overly broad and not supported by the reference.

Accordingly, applicants respectfully submit that the Examiner erred in interpreting Hamilton. Specifically, the Examiner erred in finding that the access tool is connected BETWEEN the local area networks and the one or more programmable logic controllers. This assertion is not supported by the reference, since the reference is clear that the access tool is connected BY the network to the one or more programmable logic controllers. Additionally, the Examiner erred in finding that the access tool "isolates the one or more programmable logic controllers from the local area network". The Access tool cannot possibly perform this function since the programmable logic controllers are connected to the local area network and, hence, are not "isolated" from the local area network by the access tool. Finally, the Examiner erred by interpreting the client component as a "management program" since the client component, standing alone and without interaction with the access tool, would not be capable of being used by a user to access the one or more programmable logical controllers over the local area network. Rather, both the client side and access tool are required to enable the user to access the programmable logic controllers on the network. Thus, the Examiner's interpretation of Hamilton was erroneous on several levels and this erroneous interpretation contributed to an incorrect conclusion, under 35 USC 103, that the claims would have been obvious. Accordingly, the rejection should be reversed.

In connection with Daniely, the Examiner states that Daniely teaches a system that "would provide individual protection for each computer (e.g. PLC) against unauthorized access." This is not supported by the reference. Daniely teaches at col. 4, lines 39-52 that a security gateway 14 implements a "simple firewall" which filters packets to determine whether the packets should be allowed to enter. Specifically, the firewall reads the header and compares the information in the header with a list of rules. Daniely teaches that this functionality should be implemented at the local security device 20. (Daniely at Col. 4, lines 54-67).

Thus, Daniely teaches a system where each PC has its own firewall. Further, the local security device 20 prevents the PC from taking particular actions on the network. (Daniely at Col. 4, lines 9-12). However, neither of these aspects of Daniely relate to isolating a programmable logic controller from a local area network to prevent a person using a management program from accessing the one or more programmable logical controllers over the local area network. Daniely is silent as to whether the local security device is able to stop a person using a management program from accessing the computer.

Accordingly, neither Hamilton nor Daniely teach or suggest a security policy implementation point disposed between a local area network and a programmable logic controller, that is designed to prevent a person using a management program from accessing the programmable logic controller. The Examiner's therefore erred in rejecting claim 1 and those claims dependent thereon under 35 USC 103 since this feature of claim 1 is not shown in either reference and, accordingly, would not have been obvious over the combination of references cited by the Examiner. Thus, the Examiner's rejection under 35 USC 103 should be reversed.

Conclusion

Applicants respectfully submit that the Examiner committed legal error by rejecting the claims of this application under 35 USC 103. Accordingly, the rejection of the claims in this application should be reversed.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 141315 (Ref: 15929ROUS02U).

Respectfully Submitted

Dated: October 22, 2009

/John C. Gorecki/
John C. Gorecki, Reg. No. 38,471

Anderson Gorecki & Manaras LLP
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 264-4001
Fax: (978) 264-9119
john@gorecki.us